Data Security

INTRODUCTION

Wireless local area networks are experiencing rapid growth. A continuously changing business environment requires greater flexibility from people and their working equipment. Therefore, enterprises of all sizes are starting to realise the importance of wireless connectivity inside the office premises. At the same time, the IEEE 802.11 and IEEE 802.11b industry standards for wireless LANs have opened up new possibilities for implementing wireless LAN solutions. With new interoperable wireless LAN products on the market, all enterprises and organisations are able to enjoy the convenience of wireless LANs. Many of these enterprises handle highly confidential data, and therefore security issues are often considered to be very important.

A wireless LAN is a flexible data communication system implemented as an extension to a wired LAN within a building or campus. Using radio frequency (RF) technology, wireless LANs transmit and receive data over the air, minimising the need for wired connections. Wireless LAN provides users with mobile access to a wired LAN in its coverage area. Wireless LAN has recently gained popularity in a number of vertical markets, including health care, retail, manufacturing, warehousing, and universities. These industries have profited from the productivity of using handheld devices and laptop computers to transmit real-time information to centralised hosts for processing. The demand to use LAN facilities wherever you are, and to work without complicated installations and cables, is also increasing in the everyday office environment. Standardisation of wireless LAN technologies makes it more attractive to extend or replace a part of a traditional LAN with a wireless solution.

When planning networking architecture, security issues should be carefully considered and all necessary security measures should be taken to ensure the confidentiality and integrity of data in both wired and wireless local area networks. Unlike telecommunication networks, LAN networks with IP traffic and access to the public Internet do not provide high reliability or guarantees of security. Without adequate precautions, any LAN, wired or wireless, may be vulnerable and subject to security risks and problems. For example, network data can be accessed or even altered by a hostile outsider who wishes to cash in by selling confidential business information to competitors. In the last couple of years, these risks have been complicating the full-scale use of wireless LANs containing confidential data, because users typically have strict requirements and policies for security and data integrity.

OVERVIEW OF DATA SECURITY

Security threats

Computer systems and networks face severe security threats, which may cause serious damage to a system, its services, or its information. A *security attack* is an action that compromises the security of information owned by a company, whereas a *security threat* is the possibility of execution of such an attack. Some commonly known threats are denial of service, interception, manipulation, masquerading, and repudiation.

Denial of service means that a system or network becomes unavailable for authorised users, or that the communication is interrupted or delayed. This situation could be caused by overloading a network with illegal packets, for example. In the case of wireless LAN, it can be caused by deliberate interference to operating radio frequencies, which disturbs the wireless network.

Interception can mean *identity interception*, in which the identity of a communicating party is monitored for the purposes of later misuse, or it can refer to *data interception*, in which an unauthorised user monitors user data during a communication session. This is an attack on confidentiality, and an example would be where an attacker listens in on the wireless - or wired - medium and captures the transmitted data.

Manipulation refers to a situation where data is replaced, inserted, or deleted in a system. This is an attack on data integrity and can be either unintentional (due to a hardware error) or intentional, where an attacker listens in on data communication and modifies user data.

Masquerading takes place when an attacker pretends to be an authorised user in order to gain access to information or to a system. An example of this in a wireless LAN would be when an unauthorised user tries to gain access to the wireless network.

Repudiation means that a user denies having done something that may be harmful for the system or communication. For example, users may deny that they have sent certain messages or used a wireless LAN system.

Security services and mechanisms

In order to protect against the above security threats, various security services and mechanisms need to be used. Security services enhance the security of information system and data transmissions. Security mechanisms, on the other hand, are the active measures that are used to provide security services. Encipherment is an example of a mechanism that can be used with different security services.

Authentication is a service that confirms the identity of an entity, such as a user or a device, or confirms the originality of a transmitted message. Authentication is typically needed to protect against masquerading and modification. In current wireless systems, for example, access points need to authenticate wireless devices to prevent unauthorised access to the network. Closely related to authentication is the access control service, which limits and controls access to network systems and applications. Entities must first be identified, or authenticated, before granting them access to a system.

Data confidentiality is the protection of transmitted data from interception. In wireless communications, this could mean that the data transferred between a wireless device and an access point in the air interface is kept private. Naturally, not all data is considered confidential, but critical information should not be transmitted unless security measures have been taken.

Data integrity is an important security service that proves that transmitted data has not been tampered with. Authenticating the communicating parties is not enough if the system cannot guarantee that a message has not been altered during transmission. Data integrity can be used to detect and protect data from being manipulated.

Non-repudiation prevents an entity from denying something that actually happened. This usually refers to a situation where an entity has used a service or transmitted a message, and later claims to not have done so.

SECURITY AND IEEE 802.11

Various security protocols and solutions exist that enable the protection of transmissions in computer networks. These can also be applied to wireless LANs where traffic needs to be protected from eavesdroppers. This section introduces the solutions that can be used to solve security problems in wireless LANs.

The IEEE 802.11 wireless LAN standard was ratified in 1997. The standard was developed to maximise interoperability between different brands of wireless LAN products as well as to introduce a variety of performance improvements and benefits. The IEEE 802.11 standard defines three PHY layer options: FHSS, DSSS, and IR. DSSS has some benefits compared to the other two PHY layer options. DSSS has the highest potential data rates (up to 11 Mbit/s), and it provides a greater coverage area than the FH and IR options. DSSS systems were originally used in military communication. DSSS-based radio systems are also very robust against interference.

The existing IEEE 802.11 wireless LAN standard defines two authentication services:

- Wired equivalent privacy (WEP) based shared key authentication
- Open system authentication (simply announces that a wireless device desires to associate with another wireless device or access point)

Wired equivalent privacy – WEP

The stations in an IEEE 802.11 wireless LAN can prevent eavesdropping by implementing the optional WEP algorithm, which is also used in the shared key authentication scheme. The WEP algorithm utilises the RC4 algorithm with an up to 128-bit secret key. When the wireless devices in a wireless LAN wish to communicate using WEP, they must have the same secret key in possession. The standard does not dictate how the keys are distributed to the wireless devices.

From a cryptographic point of view, the key length and the protection provided by the algorithm are important, whereas from a systems architecture point of view, the manner in which the WEP keys are distributed and managed is essential since security is based on keeping the secret keys unexposed. WEP expects that the shared secret key be delivered to all wireless devices ahead of time in a secure manner. For example, the keys can be loaded into their management bases when setting up access points and wireless devices. The advantage of using WEP is that traffic is encrypted already on the link layer between the wireless devices, so no upper layer encryption mechanisms are needed. The algorithm can be incorporated into the hardware card so that encryption is faster than with software solutions.

Open system authentication

To restrict access to a wireless network without WEP, most wireless LAN product vendors have implemented an access control method, which is based on blocking associations from unwanted MAC addresses on the access points. Wireless LAN cards have a 48-bit MAC address that uniquely identifies them as defined in IEEE 802. A list that contains the MAC addresses of valid wireless LAN cards can be defined in the access points, and any wireless device trying to associate with a wireless LAN card whose MAC address is not on the list, is denied association and thus cannot use the wireless LAN interface. If no authentication or encryption methods are used, the wireless LAN can create a security risk if the radio signals flow outside the office building. An intruder who knows the SSID (Service Set Identifier)that identifies the wireless LAN network could configure a wireless device to operate on the same network and frequency as the access points and gain access to the network if no MAC address blocking were used. With the proper tools, the intruder could eavesdrop on the data that legitimate users transmit. It is also possible to counterfeit MAC addresses used on the wireless LAN cards so that after learning an authorised MAC address, an intruder could program a wireless LAN card to have the same MAC address, and gain access to the wireless LAN. Using the wireless LAN card at the same time would of course lead to networking problems.

VIRTUAL PRIVATE NETWORKS

Virtual private network (VPN) technology can be utilised in wireless LAN networks to create virtual tunnels for secure communications. Assuming that a VPN is accurately configured, these virtual tunnels ensure that only authorised people may access the company network and that no outsider is able to read or alter the data. There are various technical approaches and standards used in implementing virtual private networks. In all of the approaches, the security content is generally distinguished by two main components: user authentication and data encryption.

User authentication

Reliable user authentication methods are essential in the wireless LAN environment. Until recently, authentication has often been based on a user ID and password, challenge response, or a central user policy database. An example of a central user policy database is the RADIUS (Remote Authentication Dial-in User Service) protocol, which is used for transmitting authentication queries by using a fixed user ID and password. RSA Security's SecurID card provides another method of authentication. SecurID is hardware that creates unique, one-time, unpredictable access codes. The access code can be used together with a secret personal PIN code to provide strong authentication. There are also many new modern methods of user authentication. Smart cards with a microcontroller and memory may contain a set of applications ranging from a simple authentication algorithm to e-cash. Smart cards provide an easy way for users to carry an authentication device with them.

Data encryption

Data encryption is used to protect data from unauthorised users by encoding its contents. Many encryption methods can be used, which differentiate themselves mainly by their encryption algorithms. Public key algorithms such as RSA use different mathematically related keys for encryption and decryption. Secret key algorithms such as RC4, DES, and 3DES use the same key for both encryption and decryption. Secret key methods are fast, but since the same key is used for encryption and decryption, data security can be endangered if key management is not reliable. The effectiveness of the encryption depends largely on key management and key length. The key must be long enough, and in modern solutions, it should exceed the minimum requirement of 56 bits.

IPSEC – The Internet protocol security standard

IPSEC is a new security standard that consists of components that provide various security services at the IP layer, such as authentication and encryption. The IPSEC standard was released in 1998 by IETF (Internet Engineering Taskforce). IPSEC can function in two different ways. In the transport mode, the original IP addresses are incorporated into the data packet and only the payload is encrypted. In the tunnel mode, the original IP addresses are also encapsulated and a new header is added to the packet. Security association (SA) is the basis for the IPSEC standard. SA is formed between communicating hosts and specifies, for example, the encryption and authentication algorithms utilised, key management properties, and the lifespan of encryption keys and the security association. One of the main topics in IPSEC is the IKE (Internet key exchange) protocol for key management, which establishes keys for encryption. The IPSEC and IKE security standard deploys private-public key pairs. Each client / user has a private key and the network stores the corresponding public key. Preshared key-based method is also supported, where the client / user and the network share the same secret key which has been delivered to them prior to communication. In the future, IPSEC will standardise the method in which data protection is carried out, and it is expected that all major hardware and software manufacturers will launch IPSEC-compatible products in 2000. IPSEC is anticipated to be the de facto standard security solution on the Internet. It could also be used as such in wireless LANs, thus making all security solutions and systems interoperable.

Secure connections to intranets with VPN

An alternative way to construct a wireless LAN with intranet access is to build a dedicated LAN segment in which the access points are connected. The wireless LAN segment can then be separated from the intranet with a security gateway that controls access to intranet resources.

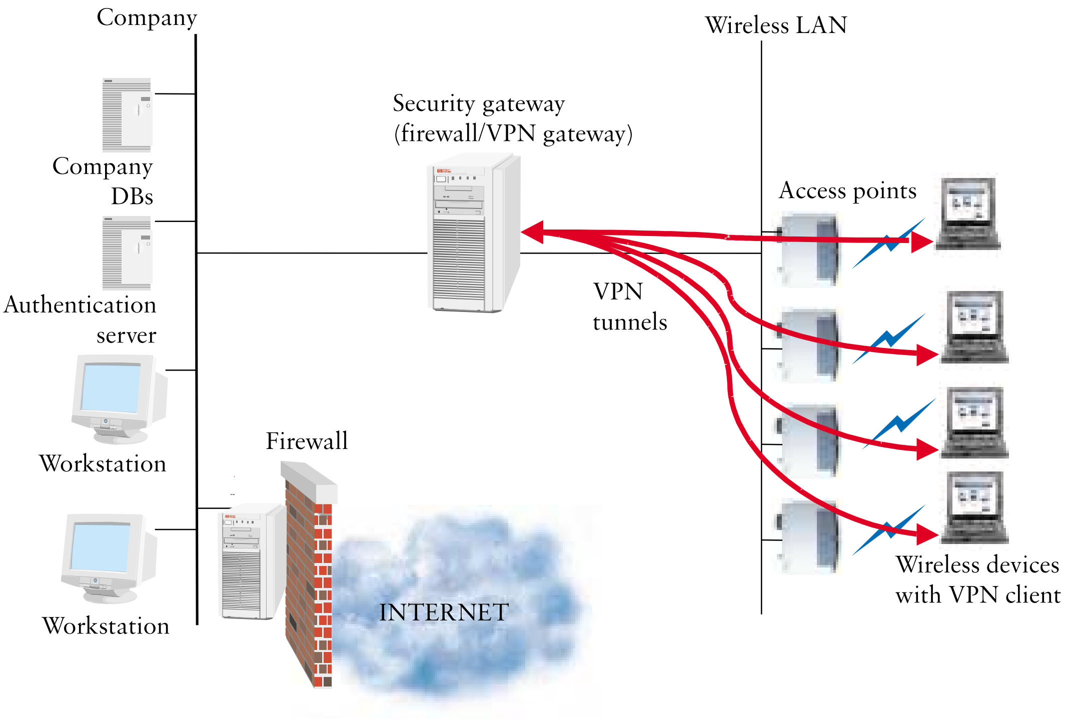

Figure 1. A wireless LAN segment in a corporation

A tunnel is created between the wireless device and the security gateway, and the data transmitted in this tunnel is authenticated and encrypted. From an implementation perspective, this setup could be based on a VPN configuration. It is possible to integrate the security gateway and the main firewall so that the wireless LAN segment is connected to the same device that is also connected to the Internet. Due to administrative reasons (and to the fact that the firewall could physically be located far away from the wireless LAN segment), however, it is better to have separate devices as depicted in the figure above.

The advantage of this solution is that it protects the information transmitted to and from the intranet, and that unauthorised access is prevented. What must be noted is that since in this model the traffic is encrypted between the wireless device and the gateway, traffic between two wireless devices in the wireless LAN segment is unencrypted unless they both use other measures, such as IPSEC (Internet Protocol Security), TLS (Transport Layer Security), or other application level encryption methods. Furthermore, the secure tunnel is established when the wireless device connects to the security gateway, so only the wireless devices can initiate connections with the intranet hosts - the intranet hosts cannot directly connect to the wireless devices.

SECURITY AND NOKIA'S WIRELESS LAN PRODUCTS

This section helps you to define an appropriate security level for Nokia's Wireless LAN products.

Nokia's 2 Mbit/s wireless LAN

The Nokia C020/C021 Wireless LAN Card and the Nokia A020 Wireless LAN Access Point do not provide any additional security options, such as WEP features.

For this reason, a complete VPN solution with strong authentication and data encryption should be used with Nokia's 2Mbit/s wireless LAN products in installations requiring a high level of security, such as in banks.

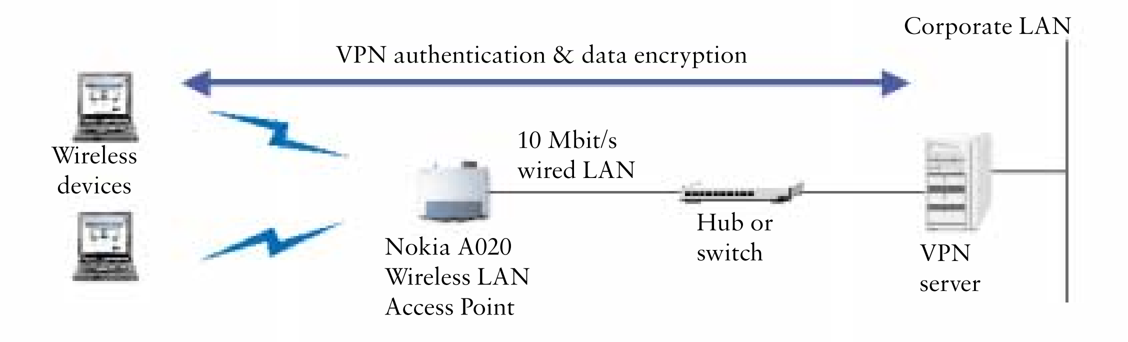
Corporate LAN
VPN authentication & data encryption
Wireless devices
10 Mbit/s wired LAN
Nokia A020 Wireless LAN Access Point
Hub or switch
VPN server

Figure 2. Example of VPN authentication in a wireless LAN

You can increase security by using NID (Network Identifier) lists in certain access points or in all of them. This prevents unauthorised, outside users as well as internal users from using certain access points.

Access point configuration and monitoring can be blocked by using the access point's lock feature and also by limiting the number of managers who are able to configure and monitor the access point (maximum 4 managers). It is also possible to define which IP addresses are allowed access. There are also options for changing ports and limiting Telnet, Web, and TFTP usage.

Nokia's new 11 Mbit/s wireless LAN

The new Nokia C110/C111 Wireless LAN Card provides additional features to increase wireless network security. First of all, it features an embedded smart card reader, which offers a highly reliable and efficient tool for managing user identities. Secondly, the solution includes wireless LAN WEP authentication & radio link encryption. In security-critical bank installations, it is still recommended to integrate the wireless LAN network with a VPN solution. However, the integrated smart card may be utilised for storing VPN level user identities and even network logon passwords.

Why use WEP? WEP may be applied to increase the network security level. First of all, it increases radio interface security both on the authentication and encryption side. Secondly, it makes cost-effective, easy to set up solutions possible. WEP allows the secure transfer of data between wireless devices. WEP offers an additional authentication and data encryption tool, which can be used as such in many installations.

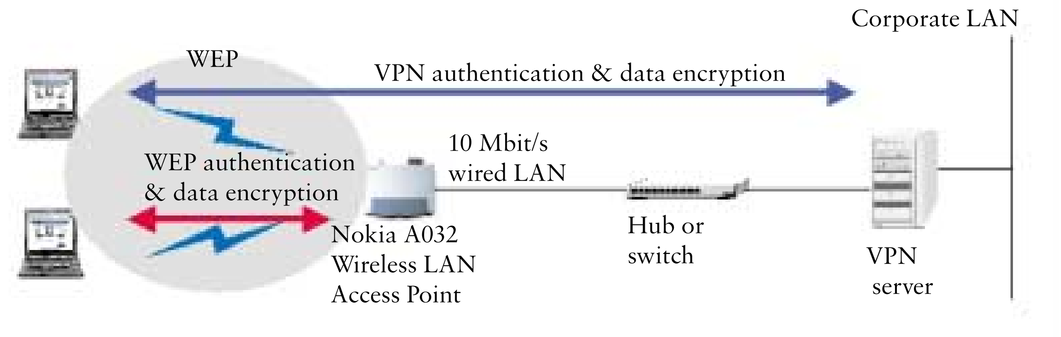
Corporate LAN
WEP
VPN authentication & data encryption
10 Mbit/s wired LAN
WEP authentication & data encryption
Nokia A032 Wireless LAN Access Point
Hub or switch
VPN server

Figure 3. Example of VPN & WEP in a wireless LAN

What about the smart cards? Nokia's integrated wireless LAN smart card reader provides an efficient tool for managing user identities and user authentication in the wireless network. Nokia's wireless LAN card offers a standard, ID000 sized Windows smart card reader interface which supports a range of commercial smart card solutions related to corporate network and service authentication.

The Nokia C110/C111 has an open smart card reader interface that supports most of the VPN solutions on the market and even allows for the development of customer-tailored smart card solutions for mobile users. The embedded smart card reader supports standard Microsoft® smart card API (Application Program Interface).

The embedded smart card reader also provides an efficient way to start applying electronic signatures. With the Nokia C110/C111 you can start using PKI-based (Public Key Infrastructure) strong authentication products alongside another security solution. We see increasing numbers of financial and other institutions starting to use PKI. In this respect, the Nokia C110 offers a sound solution for increased security demands.

The main benefits of the smart card approach are:

- A smart card provides a tangible, reliable way to distribute network authentication keys to mobile users. In addition, it provides PIN-protected storage for passwords.
- A smart card may be efficiently integrated with network authentication by using existing corporate network authentication products.
- In the future, the integrated smart card enables digital signatures and PKI services, which are becoming common especially in the banking sector.
- The integrated smart card reader allows a cost-efficient solution for providing smart card services to laptop computers.

QUESTIONS AND ANSWERS

Q1: How is the user authenticated and how is data encrypted between a wireless LAN device and an access point?

The existing IEEE 802.11 wireless LAN standard defines two authentication services:

- Open system authentication (simply announces that a wireless device desires to associate with another wireless device or access point).
- Wired equivalent privacy (WEP) based shared key authentication

In open system authentication, only valid wireless LAN cards can associate with access points. Open system authentication does not provide packet-based authentication or any data protection.

To offer frame transmission privacy, IEEE 802.11 defines optional WEP. WEP is symmetric encryption and it helps to avoid disclosure to eavesdroppers. Key lengths up to 128 bits are possible with Nokia's 11 Mbit/s wireless LAN products and the WEP mechanism encrypts all user data packets using the RC4 algorithm.

The new Nokia C110/C111 Wireless LAN Card with WEP authentication & encryption prohibits undesired users from utilising network services and provides user data scrambling over the air link. In installations requiring a high level of security, network and user data privacy can be improved by deploying IP level security mechanisms, such as VPN products. In this case, the wireless LAN network segment is isolated from the enterprise network using a VPN device. The VPN device performs user authentication and data encryption between the wireless terminal and the network using powerful encryption algorithms, such as DES or 3DES. The Nokia Wireless LAN solution supports leading VPN solutions that are transparent to the wireless LAN.

Q2: Is the radio link vulnerable to spectrum attacks?

The direct sequence spread spectrum version of the IEEE 802.11 standard is designed in such a way that it is robust against interference. However, it should be noted that no commercial wireless LAN system copes well with intentional jamming.

Q3: How can we make sure that each wireless device has a boot time password and idle session logout?

The access point terminates the authentication after a certain period of time if the wireless device is powered off or moves out of range.

The Nokia C110/C111 Wireless LAN Card offers WEP authentication, which utilises a WEP key as the boot time password. The wireless LAN as such does not guarantee any timer-based logout, but is rather seen as a normal LAN network for that kind of application.

If a reliable idle session logout and boot time password is required, it is recommended to integrate the wireless LAN with a VPN product that typically provides these features.

Q4: Is it possible to deny access to the wireless LAN on a node by node basis?

Yes. There are two complementary options: It is possible to utilise NID lists in wireless LAN access points. In this case, the access points allow only the listed wireless LAN cards (MAC address) to enter the network. NIDs limit the usage of the radio network based on the wireless LAN card MAC address. In installations where a high level of security is required, we recommend the deployment of a stronger authentication method based on a VPN solution in order to minimise the risk of network intrusion. However, in critical solutions it is possible to apply both wireless LAN and VPN level authentication. In this solution, wireless LAN authentication provides the first shield that must be cracked before getting access to hack the VPN firewall.

Q5: How does the wireless LAN affect security issues in corporations?

This completely depends on company policy. The wireless LAN radio network will definitely bring a new dimension to the security field but as always, proper planning will help to avoid possible problems. In security-critical applications, we strongly recommend the isolation of the wireless LAN network from the critical network components using a VPN firewall solution. However, unlike most competing products, Nokia's 11 Mbit/s wireless LAN card offers two advanced security tools which may be integrated with existing corporate network security systems: smart card based user authentication and wireless LAN WEP authentication and data encryption.

WEP protection provides additional shelter against intruders. The integrated smart card reader allows the network administration to easily distribute tangible user identities and secure keys to wireless LAN terminals. The smart card also provides PIN-protected password storage and allows the calculation of one-time password tokens, which is a significantly safer solution than widely deployed static passwords.

For updated information about Nokia's wireless LAN products and data security, visit our home page at www.forum.nokia.com on a regular basis.